A Practical English Auction with One-time Registration

Kazumasa OMOTE† and Atsuko MIYAJI†

School of Information Science
Japan Advanced Institute of Science and Technology,
Asahidai 1-1, Tatsunokuchi, Nomi, Ishikawa, 923-1292 JAPAN
E-mail: {omote, miyaji}@jaist.ac.jp

Abstract. An English auction is the most familiar type of auctions. Generally, an electronic auction has mainly two entities, the registration manager(RM) who treats the registration of bidders, and the auction manager(AM) who holds auctions. Before starting an auction, a bidder who wants to participate in English auction is registered to RM with her/his information. An electronic English auction protocol should satisfy the following nine properties, (a)Anonymity, (b)Traceability, (c)No framing, (d)Unforgeability, (e)Fairness, (f)Verifiability, (g)Unlikability among different auctions, (h)Linkability in an auction, and (i)Efficiency of bidding. Furthermore from the practical point of view we add two properties (j)One-time registration and (k)Easy revocation. A group signature is adapted to an English auction in order to satisfy (a), (b), and (f)[18]. However such a direct adoption suffers from the most critical drawbacks of efficiency in group signatures. In this paper we propose more realistic electronic English auction scheme, which satisfies all of these properties. Four notable features of our scheme are:
(1) both of bidding and verification of bids are done quite efficiently by introducing a bulletin board,
(2) anonymity for RM, AM and any participant can be realized to plural auctions by only one-time registration,
(3) RM can easily revoke a bidder, and
(4) nobody can impersonate any bidder.

keywords: anonymity, signature of knowledge, bulletin board, easy revocation

1 Introduction

1.1 Background

An English auction is the most familiar type of auctions. In an English auction, each bidder offers the higher price one by one, and finally a bidder who offers the highest price gets a good. An English auction is used on the Internet as well as the real world. In an English auction through the Internet, it is important to spoil

the collusion of bidders, because Internet makes the formation of ring members much easier[15]. Therefore anonymity plays an important role in spoiling the collusion of bidders. In an English auction, all bid information is published. Therefore the competition principle well works and any bidder easily knows her/his market price position. This is why an English auction is the most familiar style of auctions. In this paper, we investigate an electronic English auction.

Generally, an electronic auction has mainly two entities, the registration manager(RM) who treats the registration of bidders, and the auction manager(AM) who holds auctions. Before starting an auction, a bidder who wants to participate in English auction is registered to RM with her/his information. As for studies about an electronic auction, a sealed-bid auction has been often investigated[19, 11, 21, 22, 24, 14, 10, 3, 17, 13]. A sealed-bid auction is that each bidder secretly submits a bid to AM only once, and a bidder who offers the highest price gets the goods. A sealed-bid auction has two problems, (1)the competition principle does not work well; (2)a winning bid may be much higher price than market one.

In the case of sealed-bid auction, any canceled bid does not affect the valid bidders. However, in the case of English auction, any bid does not allow to be canceled. If a bid can be canceled in an English auction, the highest bid may be insignificant. Therefore, in an electronic English auction, it is the most important to satisfy the following two properties, (a)Anonymity and (b)Traceablitiy. Although any bidder can participate anonymously, it is necessary to identify a winner after a bidding. This means that every bid placed in an English auction must be verified maintaining the bid anonymity. Addition to the above two properties, an electronic English auction should satisfy the following nine properties:

(a) **Anonymity:** nobody can identify a bidder from her/his signature on a bid.
(b) **Traceability:** A winner cannot deny that she/he submitted the winning bid after the winner decision procedure.
(c) **No framing:** nobody can impersonate a certain bidder.
(d) **Unforgeability:** nobody can forge a bid with a valid signature.
(e) **Fairness:** all bids should be fairly dealt with.
(f) **Verifiability:** anybody can verify a signature on a bid and can confirm whether the bidder is valid or not.
(g) **Unlinkablity among different actions:** nobody can link the same bidder's bids among plural auctions.
(h) **Linkability in an auction:** anybody can link which bids are placed by the same bidder and knows how many times a bidder places a bid in an auction.
(i) **Efficiency of bidding:** the computation and communication amount in both bidding and verifying a bid is practical.

1.2 Related Works

Only a few studies on English auction[18, 23, 15, 16] have been reported as long as we know. On the other hand, many studies on a sealed-bid auction[19, 11, 21, 22,

24, 14, 10, 3, 17, 13] have been proposed because it can realize fairness more easily than English auction of public auction. These studies[15, 16] do not concern with the security aspect of public auctions but describe those different methods. [23] also proposed an electronic English auction using reverse hash chains[20] as a bid, which is similar to multiple sealed-bid biddings in order to satisfy fairness. When a bidder participates in an auction, it has two advantages that a valid bidder can place a bid many times by using only one-time signature and that bidder fairness is satisfied for a non-trusted center. However, in this protocol, the following two problems exist:

1. Anonymity for AM is not satisfied after each bidding since AM knows the bidder's identity.
2. The bidding points are set up discretely. For n bidding points, it is necessary for a bidder to compute hash functions n times. Apparently each bidder cannot place a bid as she/he likes.

[18] proposed an electronic English auction, which keeps a bidder privacy using a slightly modified group signature scheme[7, 5, 6]. So this protocol suffers from the following drawbacks of group signature schemes. In their scheme, a group manager (GM) works as AM and a group member corresponds to a bidder.

The first problem, which is the most serious, is rather complicated signature generation and verification procedure. In [7, 5, 6, 1], a membership certificate is used to reduce the data size of public group key[4]: only a group member has the certificate issued by GM. When each member generates a signature on this certificate and a bid, she/he is required the proof of the knowledge. However the proof of the knowledge needs enormous modular multiplication. In an English auction, signature generation or verification corresponds to bidding or verification of bids respectively, both of which are required in each bidding. In an electronic auction, reducing the computation amount of both signature generation and verification are much concerned compared with reducing the group public key size. Therefore we realize an electronic English auction with both fairly simple bidding and verifying procedures by introducing a bulletin board, which is usually used in putting each bid. The important feature of a bulletin board is that anybody can check the correctness of the board easily. In our protocol, the computation amount for both bidding and verifying a bid can be reduced by using a feature of bulletin board.

The second problem is anonymity. The group signature does not satisfy anonymity for GM at all since GM has a special authority. However, in an electronic auction, any bidder surely desires that nobody knows how much she/he wants to buy goods. Therefore, we need a technique of Escrow scheme[12], in which introduces Identity Escrow Agency(EA) in order to enhance anonymity for GM. This scheme realizes the perfect separability between GM and EA: only EA can identify a user by himself. This means that, in a sense, anonymity for EA is not satisfied at all. In an electronic auction, it is required that neither AM(GM) nor RM(EA) can identify the bidder from a signature on a bid, but cooperation of both parties can certainly recover the identity. In our protocol,

neither only AM nor RM identify any bidder but RM can open the signature on a bid with the help of AM and can identify the bidder. Even if a winner is identified in an auction, the winner bidder can participate in the next auction maintaining enough anonymity for both RM and AM satisfied.

The third problem is that it is rather difficult to revoke a bidder since a membership certificate is distributed to each bidder indicated in [2]. Revocation of bidder is necessary when a bidder wants to withdraw from an auction or RM wants to revoke a certain bidder. Therefore RM should be able to revoke a bidder easily. In our protocol, a revocation of bidder is done easily by using a bulletin board: just remove her/him on it.

1.3 Our Result

We propose a practical anonymous electronic English auction protocol satisfying the above eleven properties, (a)Anonymity (b)Traceability, (c)No framing, (d)Unforgeability, (e)Fairness, (f)Verifiability, (g)Unlikability among different auctions, (h)Linkability in an auction, (i)Efficiency of bidding, (j)One-time registration, and (k)Easy revocation. Our protocol satisfies both (a) and (b) simultaneously by using a combination of both the signature of the knowledge and two kinds of bulletin boards. In particular, the computation amount of both bidding and verifying each bid is fairly reduced by introducing a bulletin board. In our protocol, there are two managers RM and AM. RM manages the correspondence of bidder identity to public key, and can identify a winner or a faulty bidder with the help of AM. When a certain bidder is identified after a winner decision procedure or later disputes, AM has only to request RM to identify the bidder.

Notable features of our scheme are as follows:

- both of bidding and verification of bids are done quite efficiently by introducing a bulletin board.
- Any bidder can participate in plural auctions by only one-time registration. Even if a bidder is identified as a winner, she/he can participate in the next auction without repeating registration, maintaining anonymity for RM, AM, and any bidder.
- RM can easily revoke a bidder.
- Even if both RM and AM collude, they cannot impersonate any bidder.

The remaining of this paper is organized as follows. Section 2 summarizes a basic scheme[18] using group signature. Section 3 describes our protocol in detail. Section 4 considers fairness. Section 5 investigates the properties of our scheme.

2 Related Work

Here we summarize a previous English auction scheme[18] which uses an idea of group signature.

2.1 Group Signature

The concept of group signature was introduced by Chaum and van Heyst[8]. Group signature allows any member to sign on behalf of a group and keeps the member identity secret. The work[7] is the first efficient group signature schemes in that the size of both group's public key and of signatures are independent of the number of group members and that a group's public key remains unchanged if a new member is added to a group. Later, group signature schemes with improved performance and better flexibility are proposed in [5, 12, 6, 1]. [18] is based on these group signatures [7, 12, 5, 6].

In an English auction, GM works as AM and a group member corresponds to a bidder. When a bidder places a bid, she/he generates a group signature on a bid. The validity of signature can be verified easily by any participant using a group public key, but any participant does not know who places the bid.

2.2 Previous Scheme

Setup: AM computes an RSA modulus n, where n is the product of two primes, an RSA key pair (e, d), a cyclic group $G = \langle g \rangle$ of order n over the finite field $\mathbf{Z}_p$ for a prime p, an element $a \in \mathbf{Z}_n^*$ that is of the order $\phi(n)/4$, and an upper bound λ on the length of the secret keys: a revocation manager chooses $h \in G$ with order n, computes ElGamal-encryption key pair $(\rho,\ Y_R(= h^\rho)) \in \mathbf{Z}_n \times G$, and sets a constant $b \neq 1$. The group public key is $\mathcal{Y} = (n, e, G, g, a, \lambda, h, Y_R)$. AM's secret key is d and a revocation manager's secret key is ρ.

Registration: Alice randomly generates a secret key $x \in \{0, \cdots, 2^\lambda - 1\}$ and sends the value $y = a^x \pmod n$ and $z = g^y$ to AM; AM returns $v = (y + b)^d \pmod n$. Note that AM cannot see the value of x.

Bidding Phase: In order to put a bid m with her signature, she computes the following values $(d_1, d_2, V_1, V_2, V_3)$:

- $\tilde{g} = g^r$ and $\tilde{z} = \tilde{g}^y$ for $r \in_R \mathbf{Z}_n$;
- $d_1 = Y_R^u g^y$ and $d_2 = h^u$ for $u \in_R \mathbf{Z}_n$;
- $V_1 = SK[(\gamma, \delta) : \tilde{z} = \tilde{g}^\gamma \wedge d_2 = h^\delta \wedge d_1 = Y_R^\delta g^\gamma](m)$;
- $V_2 = SK[(\beta) : \tilde{z} = \tilde{g}^{a^\beta}](V_1)$;
- $V_3 := SK[(\alpha) : \tilde{z}\tilde{g}^b = \tilde{g}^{\alpha^e}](V_2)$

The notation of a signature of knowledge $(x_1, \cdots, x_k)$ on a message m is as follows:

$$SK[(x_1, \cdots, x_k) : z_1 = f_1(x_1, \cdots, x_k) \wedge \cdots \wedge z_\ell = f_\ell(x_1, \cdots, x_k)](m).$$

The secrets $x_1, \cdots, x_k$ satisfy all ℓ statements: $z_1 = f_1(x_1, \cdots, x_k), \cdots, z_\ell = f_\ell(x_1, \cdots, x_k)$. Assume that computing the discrete logarithm, the double discrete logarithms and the e-th root of the discrete logarithm is infeasible. The concrete algorithm for these signatures is referred to [7]. Alice's group signature consists of a set of $(d_1, d_2, V_1, V_2, V_3)$. If the signature (V_1, V_2, V_3) is valid, anyone confirms that (d_1, d_2) is an encryption of z by using ElGamal encryption function with a revocation manager's public key Y_R, and that Alice knows her secret key x and her membership certificate v.

Winner Decision Phase: A revocation manager decrypts (d_1, d_2) using his secret key ρ and identifies a member Alice from z since he knows the correspondence of z to member's identity.

In this scheme, the signature V_3 is slightly modified using a verifiable group signature sharing scheme in order to satisfy anonymity of bidder.

2.3 Undesirable Properties of the Scheme

In this scheme, there exist some problems as follows.

Efficiency: In applying a group signature to an electronic auction, it is necessary to generate or verify a signature on each bid. A signature generation or verification corresponds to bidding or verification of bids respectively, both of which are required in each bidding. However the computation amount for both signature generation and verification is rather large. Therefore it is not realistic to apply directly a group signature to an electronic auction, which requires a real-time operation.

Revocation of Bidder: In an Electronic auction, a revocation of bidder is frequently conducted when a bidder wants to withdraw from an auction or AM wants to revoke a certain bidder. So revocation-procedure should not be complicated. However, in the previous scheme, it is rather difficult to revoke a bidder since a membership certificate has been distributed to each bidder indicated in [2]. Of course, a bidder does not want to publish her/his secret key in revocation procedure. A revocation manager has to keep her/his z in a black list to revoke a certain bidder. Therefore a revocation manager can discover the unacceptable signature generated by a revoked bidder.

3 Our Protocol

In this section, we propose a practical electronic English auction.

3.1 Entities

The entities of our scheme consist of the registration manager(RM), the auction manager(AM) and a bidder($\mathcal{B}$), where each role of AM or RM is slightly different from that of previous scheme. The role of each entity is as follows:

- **RM:**
  - guarantees the correspondence of a bidder to bidder's registration key.
  - works like Identity Escrow Agency and identifies a certain bidder when AM requests.
- **AM:**
  - sponsors several auctions.
  - controls the number of a bidder's bidding in an auction.
- **Bidder($\mathcal{B}$):**
  - participates in an auction that AM holds.

3.2 Notations

Notations are defined as follows:

- p, q : two large primes ($q|p-1$)
- g : an element $g \in \mathbf{Z}_p$ with order q
- I : the number of bidders
- i : the index of bidders ($i = 1, \cdots, I$)
- $\mathcal{B}_i$: bidder i
- x_i : a secret key of $\mathcal{B}_i$ ($x_i \in_R \mathbf{Z}_q$)
- y_i : a public key of $\mathcal{B}_i$ ($y_i = g^{x_i}$) (Note that a public key is used as a registration key, and does not reveal bidder's identity.)
- r_i : AM's random number for $\mathcal{B}_i$ ($r_i \in_R \mathbf{Z}_q$)
- t_i : a random number of $\mathcal{B}_i$ ($t_i \in_R \mathbf{Z}_q$)
- T_i : an auction key for $\mathcal{B}_i$
- k : the index of auctions ($k \geq 1$)
- Y_{AM} : AM's public key ($Y_{AM} = g^{\rho},\ \rho \in_R \mathbf{Z}_q$)
- Enc : $Enc(key, data)$ is a secret key encryption function by using a secret key, key, (Note that a cipher text is uniquely determined.)
- Enc^j : $Enc^j(key, data)$ is j-times encryption by using the same key, $Enc(key, Enc(key, \cdots))$.

3.3 Procedure

Initialization: RM publishes p, q and g. AM computes a pair of public key and secret key, $(Y_{AM},\ \rho)$ using g and publishes Y_{AM}.

Bidder Registration: A bidder Alice ($\mathcal{B}_j$) registers her registration key in the following steps:

1. Alice chooses her secret key x_j and computes her registration key $y_j = g^{x_j} \pmod p$;
2. She chooses a random number t_j, named *ticket*. She uses her ticket in order to find her auction key T_j on AM's bulletin board. Note that she can also find her auction key T_j without using her ticket by checking that $y_j^{r_j} \stackrel{?}{=} (g^{r_j})^{x_j}$;
3. She sends $\{y_j, t_j\}$ to RM as her registration key, registers her identity and proves that she knows the discrete logarithm x_j of y_j to the base g by showing V_1,
$$V_1 = SK[(\alpha) : y_j = g^{\alpha}](m_R),$$
where m_R is a message published by RM;
4. When RM accepts that Alice knows the discrete logarithm, he publishes her registration key $\{y_j, t_j\}$ on his bulletin board, while RM keeps her name secretly(Figure 1).

Although Alice's name is not published at RM's bulletin board, she can easily confirm whether there exists her registration key on that board or not. Here a registration key works also as a pseudonym. We assume that RM cannot make up a secret key of a certain bidder.

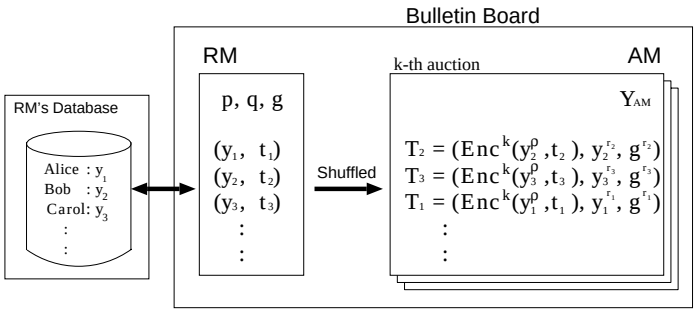

Fig. 1. Bulletin Board

AM's Setup: When a vendor requests AM to hold an auction, AM conducts the following procedure. For simplicity, here a bidder $\mathcal{B}_i$ participates in the k-th auction.

1. AM computes a shared secret key y_i^ρ with each bidder $\mathcal{B}_i$ ($y_i^\rho = Y_{AM}^{x_i}$) by using Diffie-Hellman key-distribution[9].
2. AM generates the random numbers $\{r_1, \cdots, r_I\} \in_R \mathbf{Z}_q$ for each bidder published on RM's bulletin board and keeps the numbers $\{r_1, \cdots, r_I\}$ secret.
3. AM encrypts t_i to $Enc^k(y_i^\rho, t_i) = Enc(y_i^\rho, Enc^{k-1}(y_i^\rho, t_i))$ in the k-time Enc by using a shared key y_i^ρ.
4. AM computes the following auction key T_i for $\mathcal{B}_i$ using $\mathcal{B}_i$'s public key y_i on RM's bulletin board:

$$T_i = (Enc^k(y_i^\rho, t_i),\ {y_i}^{r_i},\ g^{r_i}).$$

5. AM publishes the shuffled auction key T_i of all bidders on his bulletin board.

AM's setup has the following properties:

(A) Nobody except for AM can know the correspondence of y_i to T_i since y_i is concealed to $y_i^{r_i}$ in T_i and shuffled by AM;
(B) AM cannot identify a bidder since he does not know the correspondence of B_i's identity to y_i.

Bidding: Alice who wants to participate in the k-th auction can easily find her bidding key T_j in $\{T_1, \cdots, T_I\}$ published by AM because she knows the value $Enc^k(y_j^\rho, t_j)$ in advance by using $y_j^\rho = Y_{AM}^{x_j}$. Alice generates the signature of knowledge V_2 using both ${y_j}^{r_j}$ and g^{r_j} in T_j.

When she places a bid, she sends the following bid information $(m_j, y_j^{r_j}, g^{r_j}, V_2)$ to AM.

– a bid m_j $\quad (m_j = auction\ ID || \text{bid value})$

– $y_j^{r_j}$ and g^{r_j} (published by AM)
– $V_2 = SK[\alpha : y_j^{r_j} = (g^{r_j})^{\alpha})](m_j)$

Here V_2 implies that $\mathcal{B}_j$ knows the value of $\alpha = x_j$ if V_2 is valid signature. Furthermore both $y_j^{r_j}$ and g^{r_j} also work as a kind of certificate.

Verifiability: We assume that AM checks the validity of the signature V_2 on each bid. Of course, anybody can check the validity. If the signature V_2 is invalid signature, AM removes the bid with V_2

Checking the validity of the signature of knowledge V_2, anybody can confirm that a bidder knows surely her/his secret key. Furthermore anybody can accept that the signer is one of the bidders if the values ${y_j}^{r_j}$ and g^{r_j} in V_2 are published on AM's bulletin board.

Winner Decision: Let Alice's bid m_j be a winning bid. AM proves to RM that the public information ${y_j}^{r_j}$ added to a winning bid m_j corresponds to the registration key y_j by sending RM the value r_j^{-1}. Note that only RM can identify Alice as a winner for the first time, and that AM cannot identify a winner Alice in this winner decision.

Winner Announcement: Only the entity RM knows the winner's identity after the winner decision procedure. This means that all participants including AM cannot identify a winner but can confirm the validity of a winner. If RM informs a vendor of winner's identity after the winner decision procedure, nobody except for RM can identify a winner. Therefore anonymity of a winner is satisfied without changing her/his registration key managed by RM.

Generally, there is a problem of bidder collusion to form a ring. However, in our protocol, even if a winner Alice offers her values of bid, any bidder cannot identify her at the next auction, because AM changes r_j at every auction. Unlikability among different auctions holds in our protocol.

4 Fairness of Bidder

Fairness of bidder in an electronic auction means that any bid is fairly accepted by AM. Generally, in an electronic English auction, fairness of bidder depends on AM. There are two unfairness acts by AM:

1. AM repudiates any higher bids than a certain value.
2. AM repudiates any bidding by a certain bidder.

In order to satisfy the fairness of above 1, a bidder has to conceal a bid value for AM. As for the above 2, a bidder has to place a bid anonymously. Our protocol keeps the fairness of case 2 since bidding is done anonymously but is vulnerable to the case 1 since any value on bids is revealed. In order to avoid the case 2, we may use *non-repudiation protocol*[25, 26].

4.1 Outline of Non-repudiation Protocol

The non-repudiation protocol is that Alice sends a message to Bob and then Bob cannot repudiate a receipt of the message from Alice. We summarize the basic procedure.

1. Alice encrypts a message m into C and sends it to Bob.
2. He sends his signature $S_{Bob}(C)$ back to her after receiving C.
3. She sends the decryption key K of C to him after receiving $S_{Bob}(C)$.

Note that if Bob repudiates K after the deadline, she deposits K in TTP (Alice cannot know whether Bob repudiates K or the network between Alice and Bob is broken down). TTP publishes K using public directory service as soon as TTP receives it. Bob cannot deny receiving a message m if the network between Bob and TTP is not permanently broken down.

4.2 Bidding Procedure with Non-repudiation

Fairness of bidder is realized by introducing an idea of non-repudiation protocol as above. Non-repudiation protocol is added to a bidding procedure of our protocol. Alice and Bob correspond to a bidder $\mathcal{B}_i$ and AM, respectively. RM also plays a role of TTP. In our protocol, both RM and AM use a public bulletin board. A bid m is placed as follows:

1. AM cannot know each bid value since the bid information is encrypted by a bidder.
2. AM publishes $\mathcal{B}_i$'s signature $S_{\mathcal{B}_i}(C)$ in AM's bulletin board instead of returning it since AM does not know who is $\mathcal{B}_i$.
3. Even if AM repudiates a receipt of decryption key K from a bidder, he cannot deny getting bid information since RM publishes K in his bulletin board.

5 Consideration

5.1 Features

We discuss the following eleven properties in our protocol.

(a) **Anonymity:** nobody including either RM or AM can identify a bidder from her/his signature on a bid. Furthermore AM cannot identify a bidder though RM can identify a bidder with the help of AM. More importantly any bidder can anonymously participate in another auction by using the same registration key even if she/he has been identified once.
(b) **Traceability:** RM can open a signature on a bid with the help of AM and can identify the bidder. So a winner cannot deny that she/he has submitted the winning bid after the winner decision procedure.
(c) **No framing:** this will be discussed in chapter 5.2.

(d) **Unforgeability:** nobody can forge a bid with a signature since anybody cannot generate a valid signature using the registration key in AM's bulletin board.
(e) **Fairness:** our scheme has fairness of bidder if it applies non-repudiation protocol to bidding. Otherwise AM may decide on which bids to accept. However AM's misbehavior turn out by a bulletin board. A bidder can point out that AM does not accept her/his bid. Furthermore AM cannot identify a bidder from bids. Therefore such a dishonest act may not have an influence on electronic auction.
(f) **Verifiability:** anybody can verify the signature V_2 on a bid. Furthermore anybody can confirm whether a bidder is valid or not by checking her/his registration key in AM's bulletin board.
(g) **Unlikability among different auctions:** each bidding key generated by AM is different among each auction since AM's secret information r_i, which is different in every auction, is embedded in $y_i^{r_i}$ and g^{r_i} with a bid. So nobody except for AM can link two signatures among different auctions. Although AM can link all bids of $\mathcal{B}_j$ in all auctions, AM cannot get an identity of $\mathcal{B}_j$ except for collusion with RM.
(h) **Linkability in an auction:** a real auction has a linkability in an auction. An auction becomes active by a certain aggressive bidder who always places a higher bid. Anybody knows how many times a bidder places bids in an auction from the signature since a bidder uses both $y_i^{r_i}$ and g^{r_i} as a part of bidding information in an auction.
(i) **Efficiency of bidding:** this will be discussed in chapter 5.3.
(j) **One-time registration:** any bidder can take part in plural auctions as a valid bidder in one-time registration of registration key, maintaining anonymity for RM, AM, and any bidder.
(k) **Easy revocation:** this will be discussed in chapter 5.4.

5.2 No Framing

Here we discuss the security against framing attacks such that an entity impersonates another valid bidder.

Security against Collusion of RM and AM: Even if both RM and AM are colluded, they cannot impersonate a bidder in the following reason. In our protocol, in order to impersonate a bidder, RM and AM must show that they know the bidder's secret key x_i, which is the discrete logarithm of a part of the bidding key in AM's bulletin board. However only a bidder $\mathcal{B}_i$ knows x_i, so they cannot impersonate a bidder.

Security against RM, AM, Other Bidders, and Outsiders: In the same reason as the above, RM, AM, other bidders and outsiders cannot also impersonate another valid bidder.

Table 1. Performance for a bidder

	#Modular multiplications (1024-bit)			Communication amount (kbit)	
	Registration	Bidding	Verification	Registration	Bidding
[18]	1,500	218,600	206,700	1.3	7.6
Our scheme	480	240 (560)[1]	320 (560)	1.3	2.4

5.3 Performance

In this section, we compare our scheme with the previous scheme[18] in section 2 from the viewpoints of computation and communication amount for a bidder, which are shown in Table 2. For simplicity we estimate the computation amount by the number of 1024-bit modular multiplication and let the system parameters be $e = 3, |n| = |p| = 1024, |q| = \lambda = 160, |\mathcal{H}| = 160$ and a security parameter $\ell = 64$[7]. ¿From table 2, we see that the computation amount for a bidder is much reduced compared with the previous scheme. In particular, it is the most important to reduce the modular multiplication amount of bidding and verification, because both are conducted many times in an auction. The computation amount in our scheme is dramatically reduced by introducing two kinds of bulletin boards and an auction key. AM has only to check whether the signature V_2 is valid or not and whether there exists an auction key is in his bulletin board or not when a bidder places a bid. In this way the computation amount of both bidding and verification are reduced. Therefore our scheme can practically realize an electronic auction.

5.4 Easy Revocation

In an Electronic auction, a revocation of bidder can be frequently conducted when a bidder wants to withdraw from an auction or RM wants to revoke a certain bidder. Therefore it should be simple and easy. Furthermore the bidding history is kept secret if a bidder is revoked. In the previous scheme, it is rather difficult to revoke a bidder since a membership certificate is distributed to each bidder. In our protocol, it is easy to revoke a bidder: RM has only to delete a bidder from RM's bulletin board. Note that AM requests RM to revoke a certain bidder informing her/his information(e.g. the value r_i) or that a bidder requests RM to revoke herself/himself.

6 Conclusion

We have proposed a practical electronic auction which satisfies (a)Anonymity, (b)Traceability, (c)No framing, (d)Unforgeability, (e)Fairness, (f)Verifiability, (g)Unlikability among different auctions, (h)Linkability in an auction, (i)Efficiency

[1] This value in brackets shows the case that fairness of bidder is realized.

of bidding, (j)One-time registration, and (k)Easy revocation. Five notable features are:
(1) both of bidding and verification of bids are done quite efficiently by introducing a bulletin board,
(2) anonymity for RM, AM and any participant can be realized to plural auctions by only one-time registration,
(3) RM can easily revoke a bidder,
(4) nobody can impersonate any bidder, and
(5) Fairness of bidder can be realized.

References

1. G. Ateniese, J. Camenisch, M. Joye, and G. Tsudik. A Practical and Provably Secure Coalition-Registant Group Signature Scheme. In *Advances in Cryptology – CRYPTO2000*, pages 255–270, 2000.
2. G. Ateniese and G. Tsudik. Some Open Issues and New Directions in Group Signatures. In *Proceedings of Financial Cryptography'99*, pages 196–211, 1999.
3. C. Cachin. Efficient Private Bidding and Auctions with an Oblivious Third Party. In *Proceedings of 6th ACM Conference on Computer and Communications Security*, pages 120–127, 1999.
4. J. Camenisch. Efficient and Generalized group signatures. In *Advances in Cryptology – EUROCRYPT'97*, pages 465–479, 1997.
5. J. Camenisch and M. Michels. A Group Signature Scheme with Improved Efficiency. In *Advances in Cryptology – ASIACRYPT'98*, pages 160–174, 1998.
6. J. Camenisch and M. Michels. Separability and Efficiency for Generic Group Signature Schemes. In *Advances in Cryptology – CRYPTO'99*, pages 106–121, 1999.
7. J. Camenisch and M. Stadler. Efficient Group Signature Schemes for Large Groups. In *Advances in Cryptology – CRYPTO'97*, pages 410–424, 1997.
8. D. Chaum and E. van Heyst. Group signatures. In *Advances in Cryptology – EUROCRYPT'91*, pages 257–265, 1991.
9. W. Diffie and M. Hellman. New direction in cryptography. *IEEE Transactions on Information Theory*, pages 644–654, November 1976.
10. M. Franklin and M. Reiter. The design and implementation of a secure auction service. *IEEE Transactions on Software Engineering*, 5:302–312, 1996.
11. H. Kikuchi, M. Harkavy, and D. Tyger. Multi-round anonymous auction protocols. In *Proceedings of the First IEEE Workshop on Dependable and Real-Time E-Commerce Systems*, pages 62–69, 1998.
12. J. Kilian and E. Petrank. Identity Escrow. In *Advances in Cryptology – CRYPTO'98*, pages 169–185, 1998.
13. K. Kobayashi, H. Morita, K. Suzuki, and M. Hakuta. Efficient Sealed-bid Auction by Using One-way Functions. *IEICE Trans. Fundamentals*, E84-A(1):289–294, 2001.
14. M. Kudo. Secure electronic sealed-bid auction protocol with public key cryptography. *IEICE Trans. Fundamentals*, E81-A(1):20–27, 1998.
15. M. Kumar and S.Feldman. Internet Auctions. In *Proceedings of the Third USENIX Workshop on Electronic Commerce*, pages 49–60, 1998.
16. T. Mullen and M.Wellman. The auction manager: Market middleware for large-scale electronic commerce. In *Proceedings of the Third USENIX Workshop on Electronic Commerce*, pages 49–60, 1998.

17. M. Naor, B. Pinkas, and R. Sumner. Privacy Preserving Auctions and Mechanism Design. In *Proceedings of ACM Workshop on Electronic Commerce*, pages 120–127, 1999.
18. K. Nguyen and J. Traoré. An Online Public Auction Protocol Protecting Bidder Privacy. In *Information Security and Privacy (ACISP2000)*, pages 427–442, 2000.
19. K. Omote and A. Miyaji. An anonymous auction protocol with a single non-trusted center using binary trees. In *Proceedings of ISW2000*, pages 108–120, 2000.
20. R.L.Rivest and A.Shamir. Payword and micromint: Two simple micropayment schemes. In *Proceedings of Security Protocols*, pages 69–87, 1996.
21. K. Sako. An Auction Protocol Which Hides Bids of Losers. In *Proceedings of PKC2000*, pages 422–432, 2000.
22. K. Sakurai and S. Miyazaki. An anonymous electronic bidding protocol based on a new convertible group signature scheme. In *Proceedings of ACISP2000*, pages 385–399, 2000.
23. Stuart G. Stubblebine and Paul F. Syverson. Fair On-line Auctions Without Special Trusted Parties. In *Proceedings of Financial Cryptography'99*, pages 230–240, 1999.
24. K. Suzuki, K. Kobayashi, and H. Morita. Efficient sealed-bid auction using hash chain. In *Proceedings of ICISC 2000*, pages 189–197, 2000.
25. J. Zhou and D. Gollmann. A fair non-repudiation protocol. In *Proceedings of 1996 IEEE Symposium on Security and Privacy*, pages 55–61, 1996.
26. J. Zhou and D. Gollmann. An efficient non-repudiation protocol. In *Proceedings of the 10th Computer Security Foundations Workshop (PCSFW). IEEE Computer Society Press*, 1997.